

Tilburg University

## Tien aanpassingen aan het Nederlands procesrecht in het licht van de data-gedreven samenleving en autonome systemen

van der Sloot, Bart; van Schendel, Sascha

*Published in:*  
Tijdschrift voor Toezicht

*DOI:*  
[10.5553/TvT/187987052020011001002](https://doi.org/10.5553/TvT/187987052020011001002)

*Publication date:*  
2020

*Document Version*  
Publisher's PDF, also known as Version of record

[Link to publication in Tilburg University Research Portal](#)

*Citation for published version (APA):*  
van der Sloot, B., & van Schendel, S. (2020). Tien aanpassingen aan het Nederlands procesrecht in het licht van de data-gedreven samenleving en autonome systemen. *Tijdschrift voor Toezicht*, 2020(1), 4-13.  
<https://doi.org/10.5553/TvT/187987052020011001002>

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# Artikel

## Tien aanpassingen aan het Nederlands procesrecht in het licht van de datagedreven samenleving en autonome systemen

Bart van der Sloot en Sascha van Schendel\*

4

Nederland transformeert naar een datagedreven samenleving. De politie, de Belastingdienst en uitkeringsinstanties experimenteren met Big Data; private partijen, zoals sociale media, banken, en medische organisaties gebruiken algoritmes en profielen om beleidskeuzes te maken. Daarbij worden beleidskeuzes steeds meer geautomatiseerd. Uit de substantiële hoeveelheden data die worden verzameld worden patronen, correlaties en waarschijnlijke verbanden tussen verschillende datapunten gedestilleerd. De profielen die op basis daarvan worden vervaardigd worden gebruikt om keuzes te maken over toekomstige gevallen. Hierdoor wordt het besluit- en beleidsvormingsproces in toenemende mate gestandaardiseerd. De hoop is dat de door data-analyse geïnformeerde besluiten kwalitatief beter zullen zijn en dit de uitvoering van het beleid effectiever en efficiënter zal maken. In onderzoek dat is verricht in opdracht van het ministerie van Justitie en veiligheid wordt geconcludeerd dat tien veranderingen aan het Nederlands recht nodig zijn om deze transitie in goede banen te leiden.

### Introductie

Big Data wordt binnen steeds meer sectoren van de samenleving ingezet, een tendens die zich de komende jaren waarschijnlijk verder voort zal zetten. Om te zor-

gen voor een goede inbedding van Big Data in de publieke sector is het van belang dat er naast aandacht voor de mogelijke voordelen, zoals een efficiëntere en slagvaardigere overheid, ook wordt geïnvesteerd in het mitigeren van aan Big Data verbonden risico's en knelpunten.

Tot nu toe is er met name aandacht besteed aan de bescherming van de materiële rechten van burgers en lag de nadruk doorgaans op principes van materiële rechtvaardigheid. Zo kent de Algemene verordening gegevensbescherming nieuwe rechten toe, zoals het recht om vergeten te worden en het recht op gegevensoverdraagbaarheid. Ook besteedt zowel de literatuur als de rechtspraak aandacht aan de mogelijke negatieve gevolgen van Big Data. Vraagstukken omtrent materiële rechtvaardigheid en het toekennen van sterke materiële rechten aan burgers zijn essentieel voor een goede inbedding van Big Data in de Nederlandse publieke sector. De risico's van de datagedreven samenleving zijn zowel te zien op het gebied van mensenrechten als op het gebied van publieke waarden. Naast het recht op privacy, de diverse vrijheidsrechten en het discriminatieverbod die onder druk kunnen komen te staan met het gebruik van Big Data, is een aantal veelgenoemde risico's:

- *Chilling effect*: uit angst voor de bespiedende blik en de kans om naderhand negatieve consequenties te ondervinden van ongewenst gedrag (dat kan zijn door middel van berechting, maar ook bijvoorbeeld door sociale vormen van bestraffing, zoals uitsluiting), zullen burgers hun gedrag bij voorbaat al beperken en voldoen aan wettelijke of maatschappelijke normen.

\* Dr. B. van der Sloot is senior researcher aan het Tilburg Institute for Law, Technology and Society (TILT) van Tilburg University. S. van Schendel is promovendus aan het Tilburg Institute for Law, Technology and Society (TILT) van Tilburg University.

- *Filter bubble*: de wereld van de burger wordt gepersonaliseerd, op basis van zijn profiel. Daardoor krijgt hij dus met name informatie te zien of toegestuurd en ondervindt hij behandelingen die met dat profiel corresponderen, waardoor het wereldbeeld van de burger eenzijdiger en absoluut kan worden.
- *Mimese*: ook de negatieve aspecten van menselijk gedrag en ongelijkheid in de samenleving worden herhaald en in zekere mate versterkt. Algoritmen leren immers uit data over de reële wereld, zoals onder meer bleek bij het computerprogramma dat meediscussieerde op sociale media en al na een dag offline moest worden gehaald omdat het had ‘geleerd’ dat racistische en seksistische teksten normaal waren.<sup>1</sup>
- *Mattheus-effect*: de bestaande sociale ongelijkheid in de samenleving kan door gebruikmaking van Big Data worden herhaald en daarmee versterkt. Het gevaar dat dreigt, is dat de sterken sterker worden en de zwakken zwakker.
- *Solidariteit*: steeds beter kan worden berekend welk gedrag leidt tot welk soort risico; dat gaat dan niet alleen om de gezondheidseffecten van roken of de kans op botbreuken bij wintersport: door middel van *apps*, *fitbits* en allerhande apparaten in het *smart home* kan in feite het hele leven van mensen in kaart worden gebracht. Zo kan aan potentieel ieder gedrag consequenties worden gekoppeld. Het idee dat iedereen ook voor elkaar betaalt – de kinderloze betaalt voor kinderopvang, de niet-roker voor de medische behandeling van de roker, de man voor het zwangerschapsverlof van de vrouw, enzovoort – komt daarmee onder druk te staan.
- *Nudging*: algoritmen voorspellen niet alleen de toekomst, ze beïnvloeden die ook. Een *nudge* is een aanpassing in de keuzearchitectuur die het gedrag van mensen verandert op een voorspelbare manier zonder noodzakelijkerwijs andere opties te verbieden. Het probleem van het sturen van het onderbewuste is met name dat het de individuele vrijheid kan ondermijnen. Iemand anders stuurt die persoon immers in een bepaalde richting op basis van psychologische mechanismen. Mensen zijn zich niet noodzakelijkerwijs bewust van het feit dat ze worden beïnvloed en kunnen derhalve ook geen bewuste, vrije, beslissing nemen omtrent hun handelen.
- *Pre-emptie*: door middel van voorspellende analyse wordt geanticipeerd op gedrag van de burger dat als onwenselijk wordt gezien. Het kan de burger onmogelijk worden gemaakt dergelijk gedrag daadwerkelijk te vertonen, of er kan vroegtijdig worden ingegrepen. Big Data kan zo worden ingezet dat risico’s worden vermeden, ook als dit ten koste gaat van de autonomie van de burger.
- *Transparantieparadox*: er is bij Big Data een paradox in transparantie, kennis en macht. Door de inzet van

moderne datatechnologieën en het verzamelen van steeds meer gegevens over de burger en de samenleving en contexten waarin zij zich begeven, wordt het individu nog beter in kaart gebracht. De burger wordt daarmee dus steeds leesbaarder en beïnvloedbaarder. Aan de andere kant hebben veel burgers het gevoel dat besluitvorming door organisaties die gebruikmaken van Big Data steeds ongrijpbaarder wordt.

Minstens even belangrijk is echter dat er ook voldoende aandacht is voor de toegang tot het recht en principes van procedurele rechtvaardigheid. Burgers die wel rechten hebben maar die niet met succes kunnen afdwingen, staan immers alsnog met lege handen. Ook kunnen, als het rechtstelsel wel incidentele misstanden adresseert in specifieke gevallen, maar niet de structurele en onderliggende oorzaken, systeemfouten blijven bestaan. Dergelijke knelpunten hebben tot nu toe weinig aandacht gekregen. Dat is opmerkelijk, niet alleen omdat daardoor een aantal grotere dilemma’s onderbelicht is gebleven, maar ook omdat Big Data juist op het procedurele vlak een aantal nieuwe vragen oproept.

Daarom is in opdracht van het ministerie van Justitie en Veiligheid een studie verricht,<sup>2</sup> waaruit volgt dat het nationale en supranationale procesrecht zich momenteel kenmerkt door een sterke focus op de bescherming van de belangen van individuele rechtssubjecten in de concrete omstandigheden van het geval; het biedt met name rechtsbescherming door het toekennen van subjectieve rechten aan belanghebbenden. Dat geldt voor zowel het civiele recht, als het bestuursrecht, het strafrecht en het internationale mensenrechtenkader. Deze nadruk werkt goed voor veel traditionele rechtsgeschillen: een bouwvergunning die wordt afgewezen, een verzoek om schadevergoeding na een lasterlijke publicatie of een beperking van privacy door de overheid, waarbij iemands telefoon voor een bepaalde periode wordt afgetapt of iemands huis wordt binnengetreten door de politie. Steeds is de mogelijke inbreuk beperkt tot een specifiek persoon of een kleine groep, is de eventuele schending in tijd en ruimte af te bakenen en is het belang dat op het spel staat individueel en duidelijk bepaalbaar.

Dat ligt echter anders bij moderne mensenrechtenvraagstukken die draaien om grote gegevensverzamelingsprocessen. Big Data-projecten zijn nauwelijks in tijd, ruimte en persoon af te bakenen, maar vormen een structureel en voortdurend onderdeel van de handelingen en gedragingen van overheidsdiensten, bedrijven en burgers. De camera’s op de hoek van vrijwel iedere straat in de grote steden hebben bijvoorbeeld geen specifiek effect op één bepaald individu, ze filmen permanent eenieder die zich in de stad begeeft; een inlichtingendienst die de communicatiegegevens van een hele wijk of een stad verzamelt, raakt niemand specifiek of indivi-

1. [www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist](http://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist).

2. B. van der Sloot en S. van Schendel, *De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een datagedreven samenleving*, TILT, Tilburg University 2019, beschikbaar via [www.wodc.nl/binaries/2900\\_volledige\\_tekst\\_tcm28-402015.pdf](http://www.wodc.nl/binaries/2900_volledige_tekst_tcm28-402015.pdf).

dueel, maar iedereen gelijkelijk; de politie die door gebruikmaking van *predictive policing* in bepaalde wijken meer surveilleert dan in andere brengt daarmee geen schade toe aan concrete individuen, maar het kan wel de ongelijkheid in de samenleving in stand houden of zelfs versterken.

Dat geldt ook voor besluitvorming op basis van deze grootschalige gegevensverwerking. Moderne, datagedreven systemen gaan uit van het verzamelen van zeer grote hoeveelheden data, om daar vervolgens op algemeen of groepsniveau conclusies uit te trekken. Het vervaardigen van beleidsplannen en geautomatiseerde besluitvorming door overheidsdiensten en bedrijven op basis van deze informatie geschiedt doorgaans dan ook op groepsniveau, waarbij de groep kan verwijzen naar categorieën personen, objecten of gebeurtenissen. Steeds meer houden onder meer verzekeraars, banken, de politie en ook inlichtingendiensten bijvoorbeeld rekening met postcodegebieden en worden beleidskeuzes gemaakt op wijkniveau. Dergelijke geautomatiseerde besluitvorming vindt plaats op basis van percentages en kansen. Uit data-analyse kan bijvoorbeeld blijken dat er in wijk x een grotere kans is dat personen hun lening op tijd aflossen dan in wijk y, waarop een bank zijn beleid ten aanzien van het al dan niet verstrekken van leningen of de gevraagde rente kan afstemmen. Maar uiteraard geldt een dergelijk profiel nooit voor alle personen die in zo'n wijk woonachtig zijn. Het individu verdwijnt dus in wezen naar de achtergrond; in geautomatiseerde beleids- en besluitvorming komen de groep, de categorie en de statistische correlaties tussen datapunten steeds centraler te staan.

Meer in het algemeen is het voor dit artikel van belang dat des te groter de dataverwerkingsprocessen, des te algemener gegevensanalyse en des te vaker besluitvorming op algemene profielen en statistische correlaties zullen worden gebaseerd, des te moeilijker het zal zijn voor een individu om zijn belang concreet te maken. In wezen gaat het bij dit soort Big Data-processen vaak niet om de bescherming van individuele belangen, maar om algemene of maatschappelijke belangen. Willen we een samenleving waarin de publieke ruimte constant wordt gemonitord en waarin instanties op burgers mogen experimenteren met gedragsbeïnvloeding? Wat zouden rechtsstatelijke waarborgen moeten zijn tegen het gevaar van machtsmisbruik en geautomatiseerde besluitvorming door overheidsdiensten die veel data mogen verzamelen en welke mate van democratische legitimatie dienen dergelijke gegevensverzamelingen en besluitvormingsprocessen te hebben? Welke gevolgen heeft het personaliseren van onder meer verzekeringen en socialezekerheidsrechten voor de solidariteit in de samenleving en het draagvlak voor het spreiden van risico's? Vinden we het gerechtvaardigd om individuele burgers te beoordelen op basis van voorspellende analyses en groepsprofielen?

Daarnaast zijn bij datagedreven processen en geautomatiseerde besluitvorming procedurele vraagstukken van belang: aspecten die zien op hoe systemen en processen zijn ingericht, welke keuzes daarin zijn gemaakt

en welke gevolgen die keuzes hebben. Hoe worden data verzameld, door wie en waar en welke invloed hebben dergelijke keuzes op de mogelijke *bias* in een dataset? Welke standaarden gelden er voor algoritmen, het analyseren van datasets en de gevonden statistische correlaties in termen van kwaliteit, zorgvuldigheid en herhaalbaarheid? En welke garanties zijn er dat de datagedreven processen en geautomatiseerde besluitvorming transparant en controleerbaar zijn en dat de data-inzet aan voldoende toezicht is onderworpen?

In deze bijdrage zullen wij eerst tien meer algemene knelpunten bespreken die door de verschuiving naar een datagedreven werkwijze en geautomatiseerde beleids- en besluitvorming worden opgeroepen. Daarna zal worden besproken welke veranderingen in het Nederlands procesrecht kunnen worden aangebracht om deze knelpunten te ondervangen. Daarbij wordt zowel op het burgerlijk procesrecht, het bestuursprocesrecht, het strafprocesrecht als het constitutionele procesrecht ingegaan. Tot slot volgt een korte conclusie, met daarbij een bespreking van hoe deze mogelijke aanpassingen zich tot elkaar verhouden en in hoeverre de in dit artikel gesignaleerde knelpunten nopen tot acute actie.

## Tien knelpunten

Er zijn tien knelpunten als het huidige rechtssysteem wordt toegepast op dergelijke vraagstukken, waarbij een flink deel samenhangt met de huidige nadruk op de subjectieve rechten van natuurlijke personen om voor zijn individuele belangen op te komen.

1. *Onbekendheid*: alhoewel het individu een klachtrecht toekomt in het civiele recht en het bestuursrecht is het vaak onduidelijk voor individuen of hun data worden verzameld en door wie. Dat kan zijn omdat de operaties van dataverwerkende organisaties geheim zijn – zoals bij veiligheids- en inlichtingendiensten het geval is – of omdat data heimelijk worden verzameld – zoals bijvoorbeeld door middel van *cookies* of *device finger printing* op het internet. Als het individu niet weet dat zijn gegevens worden verzameld en eventueel worden verwerkt in Big Data-processen zal hij daar ook geen bezwaar tegen maken. Ook is het individu zich bij Big Data-toepassingen niet altijd bewust van het feit dat hij daardoor wordt beïnvloed, bijvoorbeeld omdat er gebruik wordt gemaakt van heimelijke gedragsbeïnvloeding als *nudging*.

2. *Onmogelijkheid*: duidelijk is in ieder geval dat zeer veel partijen data hebben over burgers. Schattingen lopen uiteen van enkele honderden organisaties tot enkele duizenden. Dit aantal zal met de komst van Big Data vermoedelijk alleen maar groter worden. Daarbij geldt dat het voor het individu ondoenlijk is om bij al die partijen na te gaan of zij gegevens over hem hebben, of zij die legitiem verwerken en zo niet, om een klacht in te stellen bij een rechter of een handhavingsorganisatie.

3. *Ongelijkheid*: daarbij komt dat de partijen die experimenteren met Big Data-processen doorgaans grote internetgiganten zoals Google, Facebook en Apple of overheidsdiensten zijn. Als het komt tot een rechtszaak, dan staat het individu doorgaans zwak tegen deze zeer bemiddelde en grote organisaties.

4. *Geen specifiek, individueel belang*: ook is het vaak onduidelijk in hoeverre een individu nu wordt geraakt door een bepaalde Big Data-toepassing, bijvoorbeeld welke schade hij heeft geleden of welk belang wordt ondermijnd. In het recht is traditioneel vereist dat degene die een klacht indient een belang heeft dat te onderscheiden valt van de amorfe massa. Toch hebben veel van de Big Data-toepassingen invloed op de hele bevolking of zeer grote groepen. De camera's op de hoek van vrijwel iedere straat in de grote steden hebben geen specifiek effect op één bepaald individu – het raakt iedereen die zich in de stad begeeft. Als de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) gebruik zou maken van de mogelijkheid om een hele wijk of een stad te monitoren wordt niemand specifiek of individueel geraakt, maar iedereen gelijkelijk. Het individuele belang als zodanig is niet direct evident. Er is niemand direct getroffen door het feit dat de politie haar zoekopdracht beperkt tot een wijk waar veel mensen met een migratieachtergrond wonen. Daarbij komt dat het huidige recht in de vorm van de Algemene verordening gegevensbescherming alleen bescherming biedt aan gegevens als die direct of indirect aan een persoon zijn te relateren. Juist in de analysefase van Big Data-processen is dat doorgaans niet het geval, omdat hier grote categorieën data op geaggregeerd niveau worden verwerkt, zonder dat de data aan een direct en concreet individu zijn gekoppeld. Meer in het algemeen wordt deze focus op 'persoonsgegevens' steeds problematischer, omdat analyses op basis van metadata of niet direct aan een individu gekoppelde gegevens steeds meer als even waardevol worden beschouwd.<sup>3</sup> Aangezien Big Data-analyses toch op hoog abstractieniveau naar verbanden zoeken is het vaak onbelangrijk of de data aanvankelijk aan een individu waren gelinkt of niet. Ook op dit punt bestaat er dus een mismatch tussen het op het individu gerichte recht en de het individu-overstijgende Big Data-praktijk.

5. *Geen persoonlijk, maar algemeen belang*: bij veel van de Big Data-problematiek zou het ook misplaatst zijn een koppeling te maken met het individuele belang. De vraag of inlichtingendiensten een bevoegdheid tot zogenoemde bulkinterceptie zou moeten toekomen is een abstracte, normatieve vraag – het verenigen van dit punt tot de eventuele belangen van een specifiek individu zou betekenen dat het eigenlijke punt wordt gemist. Net zo is het met het veelgehoorde gevaar van machtsmisbruik, machtsongelijkheid (de burger wordt steeds transparan-

ter voor de overheid, terwijl de overheid die haar keuzes op datagedreven en algoritme gestuurde profielen baseert het gevaar loopt zelf steeds moeilijker te begrijpen zijn voor de burger) en sociale stratificatie oftewel het Mattheuseffect (het gevaar dat Big Data-profielen ongelijkheden in de samenleving reproduceren en dat het beleid dat daarop wordt gebaseerd deze ongelijkheid versterkt); allemaal gevaren die vaak in verband worden gebracht met Big Data. De eigenlijke problemen van Big Data zijn doorgaans gekoppeld aan grotere, maatschappelijke vraagstukken.

6. *Eerlijk proces onder druk*: een probleem dat hieraan gelieerd is, is het recht op een eerlijk proces. Steeds meer beslissingen binnen de overheid worden genomen op basis van computergestuurde en datagedreven analyses. Vaak zijn de algoritmen die hiervoor worden gebruikt zeer complex. Het is dan vaak zeer ingewikkeld en tijdrovend voor een individu om te analyseren of een uitkomst juist is en waar een eventuele fout zou kunnen zijn gemaakt. Bij *deep learning* en zelflerende algoritmen is het zelfs voor de programmeurs lang niet altijd duidelijk hoe en waarom de computer tot een bepaald resultaat is gekomen. Hierdoor dreigt het uitgangspunt dat de overheid transparant en controleerbaar moet zijn onder druk te komen staan. Een algoritme wordt dan ook vaak als *black box* aangeduid, aangezien er weinig transparantie is ten aanzien van hoe de algoritmen werken, welke data ze wel en niet meenemen en welke aannames ten grondslag liggen aan de analyseprocessen. Data-expert Frank Pasquale stelt dat dit een kenmerkend aspect is van onze hedendaagse samenleving, die hij dan ook de *Black Box Society* noemt.<sup>4</sup> Een schrijnend voorbeeld hiervan komt uit de Verenigde Staten, waar iemand een extra lange gevangenisstraf kreeg opgelegd vanwege een computerprogramma dat de veroordeelde een hoog risico voor de samenleving achtte. De veroordeelde eiste vervolgens inzage in hoe het oordeel over hem in stand was gekomen, maar het Supreme Court van Wisconsin oordeelde hierover in zijn nadeel, om zo de bedrijfsbelangen van het bedrijf dat de risicoanalyse over verdachten maakt te beschermen.<sup>5</sup>

7. *Analysefase beperkt gereguleerd*: het recht is nog op een ander punt in sterke mate gericht op het individu. Het stelt regels voor het verzamelen van data, die aan een persoon zijn gekoppeld, onder andere door de Algemene verordening gegevensbescherming, en stelt regels aan het gebruik van de gegevens, bijvoorbeeld als er gevaar voor discriminatie of stigmatisering bestaat of personen op een andere wijze oneerlijk worden behandeld. Zowel in het begin (als de gegevens van een persoon worden verzameld) als aan het eind (als de analyses tot een beleid hebben geleid dat in de praktijk op een groep of

3. Ook niet-persoonlijke gegevens zijn thans gereguleerd: Verordening (EU) 2018/1807 van het Europees parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie, *PbEU* 2018, L 303/59.

4. F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, Massachusetts/Londen: Harvard University Press 2015, beschikbaar via <http://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf>.

5. [www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/](http://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/).



persoon wordt toegepast) is het mogelijk om een link te maken met het individu (alhoewel dit steeds lastiger wordt). De tussenfase, waarin de data worden geanalyseerd, blijft echter grotendeel buiten het bereik van de wet omdat het hier gaat om grote datasets en analyses op hoog geaggregeerd niveau. Toch is het hier dat veel van de problemen ontstaan. Zo kent de dataset vaak een *bias* of vooringenomenheid (de politie heeft bijvoorbeeld meer gesurveilleerd in de Bijlmer dan in Amsterdam Oud-Zuid), de categorisering is niet-neutraal en de algoritmen (in wezen complexe beslisbomen) gaan uit van onbewezen aannames – al deze zaken kunnen de betrouwbaarheid van de data-analyse onder druk zetten, iets wat de betrouwbaarheid van de overheid en de legitimiteit van haar beleid als zodanig onder druk zet. Er zijn geen juridische normen die eisen stellen aan de betrouwbaarheid van de Big Data-analyses.<sup>6</sup>

8. *Beleidskeuzes moeilijk aan te vechten*: daarbij kan in het huidige recht moeilijk tegen beleidskeuzes als zodanig worden opgekomen. Stel, de politie besluit op basis van *predictive policing* voornamelijk te surveilleren in de Bijlmer en minder in Amsterdam Oud-Zuid. Kan een inwoner in de Bijlmer daartegen opkomen omdat hij meent dat de database op basis waarvan de voorspellingen zijn gedaan vooringenomen is of een inwoner van Oud-Zuid die wil dat er meer gesurveilleerd wordt in zijn wijk? Kan een derde – bijvoorbeeld een persoon met een immigratieachtergrond – wiens data geen onderdeel vormen van de dataset, maar die desalniettemin onderdeel vormt van een groep waarover bepaalde conclusies worden getrokken, hiertegen bezwaar maken? Stel, de politie besluit speciale aandacht te geven aan drugsdelinquenten en besluit de beschikbare databases te doorzoeken op aanwijzingen. Daarbij beperkt zij de zoekopdracht evenwel tot personen uit een bepaalde wijk, waarin veel personen wonen met een migratieachtergrond. De resultaten die daaruit volgen, kunnen weliswaar bruikbaar zijn en er kan worden gezocht naar additioneel bewijs om te komen tot een arrestatie of eventuele veroordeling. Kan iemand tegen wie vervolgens onomstotelijk bewijs is gevonden dat hij in drugs handelt, vervolgens bezwaar maken op grond van een discriminatoir beleid? Dat zal in de praktijk moeilijk zijn, terwijl een dergelijke beleidskeuze desalniettemin kan leiden tot structurele problematiek.<sup>7</sup>

9. *Materiële rechtsbescherming beperkt*: ook de materiële reikwijdte van veel andere rechtsbegrippen die door Big Data onder druk kunnen komen te staan is in directe of indirecte wijze gelieerd aan het individu. Voorbeelden zijn de persoonlijke levenssfeer, menselijke waardigheid

en individuele autonomie, maar ook het huis en de privésfeer. Een daarbij komend probleem is dat onder meer door Big Data-projecten de afbakening tussen wat privé is en wat niet vervaagt. In het huis van de toekomst zijn steeds meer apparaten gelinkt met het internet en wordt er door apparaten constant gecommuniceerd met elkaar en met de buitenwereld. Door de introductie van *smartphones* en *cloud computing* dragen individuen een groot deel van hun privéleven constant bij zich. Het privéleven voltrekt zich niet langer primair in de woning of privésfeer van een persoon, maar overal.

10. *Verantwoordelijkheid moeilijk toe te delen*: in toeneemende mate wordt voor Big Data-analyse gebruikgemaakt van data die afkomstig zijn van andere partijen. Er is een risico dat de partij die gebruikmaakt van de uitkomst van de analyse zich probeert te vrijwaren van verantwoordelijkheid. Zo kunnen overheidspartijen proberen gebruik te maken van data-analyse uit de private sector wanneer zij de gewenste data of analysemethoden zelf niet voorhanden hebben, of kan getracht worden de verantwoordelijkheid voor fouten in de analyse door te schuiven naar de softwareontwerper. Naast het ontlopen van verantwoordelijkheid kan dit ook voor individuen onderworpen aan Big Data-analyse problemen opwerpen: bij wie moet men zijnbeklag doen, of wie moet men voor de rechter dagen? Wat als verantwoordelijkheid wordt uitgesloten en er bij andere partijen in de keten niets te halen valt?

## Tien aanpassingen aan het Nederlands procesrecht

Alhoewel het nationale en supranationale recht wel enkele mogelijkheden kennen om dit type vragen te adresseren en bescherming te bieden aan individuoverstijgende rechten en belangen, bijvoorbeeld door gespecialiseerde burgerrechtenorganisaties, zijn deze mogelijkheden vooralsnog beperkt en geven zij zich geen rekenschap van de fundamentele veranderingen die door Big Data-processen worden ingezet. Als steeds meer processen binnen de overheid datagedreven worden, dan is het belangrijk een aantal aanpassingen door te voeren in recht en beleid. Daarom hebben wij bekeken welke aanpassingen er nodig zijn voor een betere en stevigere inbedding van Big Data in de Nederlandse publieke sector. Daaruit volgen tien concrete voorstellen voor aanpassingen aan het juridisch kader, die alle zijn terug te voeren op twee kernprincipes. Enerzijds moet het Nederlandse (proces)recht meer aandacht schenken aan de bescherming van algemene en maatschappelijke belangen. Anderzijds dient het Nederlandse recht meer ruimte te bieden voor niet-natuurlijke personen, zoals burgerrechtenorganisaties, om zaken in het algemeen belang te voeren of maatschappelijke belangen in rechte te verdedigen. De tien voorstellen worden hieronder kort besproken.

6. Zie uitgebreider: B. van der Sloot, 'Beyond the access-use debate: regulating the analysis of information in the Big Data era in order to ensure reliability and trustworthiness', in: S. Goslinga e.a. (red.), *Tax and Trust. Instructions, Interactions and Instruments*, Den Haag: Eleven International Publishing 2018.

7. Zie uitgebreider: S. van Schendel, 'The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI', in: L. Reins (red.), *Regulating new technologies in uncertain times*, The Hague: T.M.C. Asser Press | Springer 2019.

## 1. Geef duidelijkheid over bewijsuitsluiting en strafvermindering

Zowel inlichtingen- en veiligheidsdiensten als opsporingsdiensten maken steeds meer gebruik van Big Data. Daarbij worden niet zelden profielen gebruikt voor de keuze waar, hoe en wanneer data worden verzameld of menskracht wordt ingezet. Zo kunnen postcodegebieden of andere algemene groepskenmerken van belang worden in de strafrechtketen. Daarnaast kunnen profielen indiceren wie verder te onderzoeken teneinde opsporingscapaciteiten zo efficiënt mogelijk in te zetten. De basis voor voorspellingen hangt echter vaak samen met statistiek en geaggregeerde data. Een voorspelling is immers niets meer dan anticiperen wat voor gedrag zal plaatsvinden gebaseerd op data van andere, vergelijkbare situaties uit het verleden. Een van de meest genoemde gevaren dat hierbij wordt gesignaleerd, zowel in de literatuur als in de voor het onderzoek gevoerde interviews,<sup>8</sup> is het risico op discriminatie en stigmatisering.

Stel bijvoorbeeld: de politie maakt gebruik van een dataset met een indirecte bias naar een bepaalde bevolkingsgroep. Op basis van een analyse van deze dataset wordt besloten tot onderzoek naar meerdere personen uit deze bevolkingsgroep en vervolgens wordt er bewijs tegen één van hen gevonden. De persoon wordt voorgeleid aan de rechter. De rechter zal oordelen dat het gevonden bewijs in principe rechtmatig en toelaatbaar is. Toch kan het maatschappelijk onwenselijk zijn als er bovenmatige aandacht is tijdens de onderzoeks- en opsporingsfase voor personen van een bepaalde bevolkingsgroep, terwijl plegers van strafbare feiten uit andere bevolkingsgroepen onevenredig minder in het vizier komen.

Tegen dergelijk overheidshandelen kan eventueel een klacht worden ingediend binnen het bestuursrecht, omdat dit handelen strijdig kan zijn met de beginselen van behoorlijk bestuur. De wetgever zou er echter voor kunnen kiezen om ook binnen het strafrecht consequenties te verbinden aan eventuele indirecte discriminatie en *bias* in Big Data-processen. Daarbij zou aansluiting kunnen worden gezocht bij de herziening van Boek 4 van het nieuwe Wetboek van Strafvordering en de regels voor bewijsuitsluiting en strafvermindering.<sup>9</sup> Het gaat bij grote datagedreven projecten dan niet zozeer om het maken van onderscheid op zich, maar om een schending

van het non-discriminatiebeginsel als een *bias* in een systeem leidt tot een schending van het recht op een eerlijk proces.

## 2. Geef rechtspersonen de mogelijkheid zich te voegen als partij in een strafzaak

Daarnaast zou met betrekking tot de besproken problematiek voor een tweede, minstens even belangrijke oplossing kunnen worden gekozen. Door de mogelijkheid van bewijsuitsluiting en strafvermindering wordt de individuele verdachte weliswaar gecompenseerd voor eventueel nadeel, het onderliggende probleem (de *bias* in de dataset of algoritme) wordt niet noodzakelijkerwijs aangepakt. Om dit euvel te voorkomen zou de wetgever de mogelijkheid kunnen geven aan burgerrechtenorganisaties om zich als partij te voegen in een strafzaak. De rechtspersoon neemt dan niet het initiatief tot een zaak tegen een verdachte noch is deze zelf de verdachte. Wel zou de organisatie zich dan in een zaak kunnen voegen om de rechter duidelijk te maken dat in het kader van het voor het strafdossier relevante onderzoek gebruik is gemaakt van Big Data-technieken die negatieve effecten kunnen hebben op het recht op een eerlijk proces, het non-discriminatiebeginsel en de betrouwbaarheid van bewijs. Zij kan expertise op dit gebied toevoegen aan de strafzaak en zo een punt naar voren brengen dat de specifieke strafzaak ontstijgt. Deze mogelijkheid is met name relevant wanneer het een structurele praktijk betreft die een uitwerking heeft op het strafrechtstelsel die verder gaat dan de individuele belangen van de verdachte of slachtoffer. Wel zou bij de eventuele introductie van een dergelijke rechtsfiguur als eis moeten worden opgenomen dat de verdachte akkoord gaat met de voeging van de rechtspersoon, zodat de rechtspersoon geen argumenten aanvoert die de verdediging van de verdachte doorkruisen.

## 3. Breid de mogelijkheden voor rechtspersonen om een strafproces te initiëren uit

Er zijn voor burgers en belangenorganisaties momenteel binnen het strafrecht vrijwel geen mogelijkheden om algemene of groepsbelangen aan de kaak te stellen. De enige optie is om een artikel 12 Sv-procedure te beginnen. Het is niet uitgesloten dat het bij Big Data-processen ook voor rechtspersonen mogelijk zou zijn om een dergelijke procedure te starten, voor zover de klacht volgt uit de statutaire doelstellingen en blijkt uit feitelijke werkzaamheden. Daarbij valt bijvoorbeeld te denken aan (culpoze) gegevensbeschadiging of het onrechtmatig overnemen van gegevens, maar ook aan discriminatie door *profiling*. Zelfs zou het kunnen voorkomen dat de overheid zelf strafrechtelijk wordt vervolgd voor schendingen van strafrechtelijke bepalingen.

Zelfs als een dergelijke procedure succesvol is, ligt het uiteindelijke vervolgingsmonopolie echter bij het Openbaar Ministerie (OM), waardoor partijen geen controle hebben over of invloed op het gevoerde proces. Dit is voor burgerrechtenorganisaties een van de belangrijkste redenen om geen strafrechtelijke procedures te beginnen in het kader van datagedreven projecten. Een nadeel van

8. Interviews zijn afgenomen met: Amnesty International Nederland (Dou-tje Lettinga en Nine de Vries), Autoriteit Persoonsgegevens (Aleid Wolfsen), Belastingdienst (Raymond Kok), Bits of Freedom (David Korteweg), Boekx advocaten (Otto Volgenant en Charlotte Hangx), Bureau Brandeis (Christiaan Alberdingk Thijm), College voor de Rechten van de Mens (Jan-Peter Loof en Juliette Bonheur), Datavakbond (Reinier Tromp), Hoge Raad (Ybo Buruma), Landsadvocaat Pels Rijcken (Cécile Bitter), de Nationale ombudsman (Reinier van Zutphen en Martin Blaakman), Privacy First (Vincent Böhre), Public Interest Litigation Project (Jelle Klaas), Radboud Universiteit (Roel Schutgens en Joost Sillen) en schrijver/publicist (Maxim Februari).

9. Voorstel van wet tot vaststelling van Boek 4 van het nieuwe Wetboek van Strafvordering inhoudende bepalingen over de berechting in verband met de modernisering van het Wetboek van Strafvordering (Vaststellingswet Boek 4 van het nieuwe Wetboek van Strafvordering (Berechting)), MvT, p. 92.

deze constellatie is dat het OM niet op alle punten de specialistische expertise heeft die deze organisaties, zoals Amnesty International, Bits of Freedom en Privacy First, wel hebben. Wil de wetgever op dit punt bredere mogelijkheden introduceren dan zou hij onder meer kunnen kijken naar het Franse rechtssysteem; onder Frans recht is er zowel een *action publique* als een *action civile* mogelijk. Zoals de naam al doet vermoeden is de publieke actie vervolging door het Openbaar Ministerie en civiele actie vervolging door een private partij. Deze private partij betreft hoofdzakelijk het slachtoffer, maar ook rechtspersonen kunnen binnen het strafrecht opkomen voor algemene belangen als zij op dat terrein gespecialiseerd zijn.<sup>10</sup>

#### 4. Introduceer de figuur van een 'special advocate'

Over het algemeen dienen partijen die werken met grote datagedreven projecten openheid te betrachten, maar er zijn evidente gevallen waarin partijen niet volledig transparant kunnen zijn over de door hen gebruikte data, algoritmen en de weging van de verschillende statistische uitkomsten, bijvoorbeeld omdat dit calculerend gedrag van burgers met zich mee zou brengen. Als de wetgever voor dergelijke situaties toch een vorm van openheid en controle zou willen bewerkstelligen dan zou hij inspiratie kunnen vinden bij de figuur van de *special advocate*, zoals die onder meer in het Britse recht bekend is.<sup>11</sup> De *special advocate* is een advocaat die een persoon verdedigt of vertegenwoordigt in rechte, maar niet is aangesteld door die persoon noch directe instructies van diegene ontvangt. De *special advocate* is bevoegd om het bewijs in te zien dat een verdachte, vaak vanwege staatsveiligheid, niet mag inzien, en kan dan namens de verdachte spreken en handelen. Deze *special advocates* zijn gespecialiseerde advocaten die een screening te hebben ondergaan en worden benoemd door de *Attorney General*.

De *special advocate* zou in Nederland kunnen worden geïntroduceerd in de Big Data-context; deze speciale advocaat zou dan toegang kunnen krijgen tot de algoritmen, inputdata en uitkomsten van analyses die niet kunnen worden vrijgegeven uit overwegingen van nationale veiligheid of redenen van de afscherming van opsporingsmethoden ter waarborging van de werking daarvan.<sup>12</sup> Naast het strafrecht zou de *special advocate* ook een rol kunnen spelen binnen het bestuursrecht. In het bestuursrecht is op grond van de recente *Aerius*-rechtszaak omtrent het PAS-systeem het uitgangspunt dat beslisregels openbaar kunnen worden gemaakt zonder het algoritme bloot te leggen en dat men zich niet achter het systeem kan verschuilen dat de beslissing

heeft genomen.<sup>13</sup> Wanneer bepaalde informatie toch niet wordt gedeeld met de betrokkene kan de rechter op grond van artikel 8:29 Awb toetsen of er een gerechtvaardigd belang is om informatie niet bekend te maken aan eiser. De *special advocate* zou in zo'n geval betrokken kunnen worden in de besluiten om informatie niet bekend te maken. De informatie zou dan met de *special advocate* kunnen worden gedeeld, die deze informatie dan niet verder met bijvoorbeeld belanghebbenden mag delen, maar wel zou kunnen toetsen of de informatie terecht buiten de procedure is gehouden.

#### 5. Stel beroepsmogelijkheden open voor voorbereidingshandelingen

Momenteel is het lastig om in het bestuursrecht feitelijke handelingen, niet zijnde een besluit, aan te vechten en geldt op grond van artikel 6:3 Awb een beperking voor bezwaar en beroep ten aanzien van een beslissing inzake de procedure ter voorbereiding van een besluit. In Big Data-processen worden op basis van risicoprofielen beslissingen genomen over vervolgonderzoek en worden feitelijke handelingen genomen, die niet noodzakelijkerwijs een rechtshandeling met zich mee hoeven te brengen. Zo kan het gaan om verdere informatievergaring door middel van huisbezoeken of *screening* op wijkniveau. Van rechtsbescherming voor een individu is onder het huidige recht pas sprake wanneer eventueel nadeel voor de betrokkene is ontstaan maar dit laat onverlet dat structurele en onderliggende problematiek kan blijven bestaan, zoals de eerder genoemde *bias* in de dataset, maar ook meer algemene problemen omtrent betrouwbaarheid en validiteit van de gebruikte data, algoritmen en de daaruit voortvloeiende profielen. Het grootste en belangrijkste deel van Big Data-processen, namelijk de fase waarin de verzamelde data worden geanalyseerd, statistische correlaties worden gevonden en groepsprofielen worden gemaakt, valt daarmee buiten de huidige juridische kaders en zelfs besluiten kunnen slechts aan rechterlijke toetsing worden onderworpen als ze een duidelijk en individueel belang voor een belanghebbende met zich meebrengen, wat zoals uitgelegd in grote datagedreven processen niet altijd evident is. Daarom kan het wenselijk zijn om ook beroepsmogelijkheden open te stellen voor feitelijke en voorbereidingshandelingen.

#### 6. Stel beroepsmogelijkheden open tegen algemeen verbindende voorschriften en beleidsregels

Zoals gezegd is het bestuursrecht momenteel sterk geënt op individuele rechtsbescherming voor belanghebbenden ten aanzien van concrete besluiten. Zo volgt uit artikel 8:3 Awb dat geen beroep kan worden ingesteld tegen een besluit inhoudende een algemeen verbindend voorschrift of een beleidsregel. Big Data-processen leunen sterk op algemene profielen en statistische correlaties, terwijl de rechtsbescherming van de Awb pas in beeld komt wanneer er sprake is van een besluit op basis

10. Art. 2-1 tot en met 2-21 Code de procédure pénale. Het gaat hierbij wel om een beperkt aantal delicten.

11. A. Boon en S. Nash, 'Special Advocacy: Political Expediency and Legal Roles in Modern Judicial Systems', *Legal Ethics* 2006, nr. 1; J. Ip, 'The Rise and Spread of the Special Advocate', *Public Law* 2008, p. 717-741, 2008, beschikbaar via <https://ssrn.com/abstract=1292537>.

12. Dit zou bijvoorbeeld kunnen worden opgenomen in een in te voegen regeling in titel III (De raadsman) van het Eerste Boek van het Wetboek van Strafvordering.

13. ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 (*Stichting Werkgroep Behoud de Peel/Gedeputeerde Staten van Noord-Brabant*).



van deze processen. Veel van de inzichten die met Big Data worden verkregen zullen echter worden gebruikt om algemeen beleid vorm te geven en om de algemene plaatselijke verordening (APV), bestemmingsplannen of andere maatregelen vast te stellen. Wederom blijft het punt dat als een dergelijke maatregel niet leidt tot een besluit, maar wel, om welke reden dan ook, problematisch wordt geacht, er weinig mogelijkheden zijn om dergelijke punten juridisch te adresseren. Om dit probleem aan te pakken kan de wetgever overwegen om toetsing van algemene beleidskaders, groepsprofielen en algemeen verbindende voorschriften mogelijk te maken, in ieder geval binnen de Big Data-context. Deze verruiming zou aansluiten bij een roep die al langer bestaat om verruiming op dit punt te bieden.<sup>14</sup>

### 7. Creëer een mogelijkheid om wet- en regelgeving in abstracto te toetsen

Terwijl het Europees Hof voor de Rechten van de Mens voorheen zaken uitsluitend *in concreto* toetste, dat wil zeggen dat de klagers concreet belanghebbenden moesten zijn en dat het Hof slechts een oordeel vormde over de omstandigheden van het concrete geval, is er de laatste tijd een kentering. Met name in zaken die draaien om de grootschalige verwerking van gegevens is het bereid om wetgeving ook in abstracto te toetsen.<sup>15</sup> Bij dergelijke *in abstracto* zaken bekijkt het Hof niet of er in een specifiek geval schade is geleden door de klagers en of die schade in de omstandigheden van het geval in verhouding stond tot het gediende algemeen belang, zoals de nationale veiligheid, maar toetst het wet- en regelgeving op algemene principes van rechtsstatelijkheid en rechtmatigheid. Hierbij kijkt het naar de 'kwaliteit van de wet'. Criteria die hiervoor gelden, zijn niet alleen of de wet helder is en voorzienbaar in haar effecten, maar ook of er voldoende waarborgen zijn opgenomen tegen machtsmisbruik, dat er transparantie wordt betracht en dat er voldoende rechterlijke en parlementaire controle op de inzet van de bevoegdheden van de uitvoerende macht is neergelegd in de wet. De eisen van legaliteit en legitimiteit van wetgeving zijn minimumvereisten. Met name in de Big Data-context is het Hof een aantal keer tot een schending gekomen.

De Nederlandse regering zou aansluiting kunnen zoeken bij deze opening, wat navolging zou geven aan een van de aanbevelingen van de commissie-Remkes.<sup>16</sup> Om een vorm van abstracte toetsing in te voeren is het niet noodzakelijk om het toetsingsverbod uit de Grondwet te schrappen, aangezien kan worden volstaan met een verwijzing naar onder meer het Handvest van de Grondrechten van de EU, het Europees Verdrag voor de

Rechten van de Mens en internationale verdragen. Wel zou de wetgever kunnen overwegen om abstracte toetsing van wetgeving als expliciete taak te beleggen bij de Hoge Raad en/of de Afdeling bestuursrechtspraak van de Raad van State. Een dergelijke toetsing zou zowel *ex ante* als *ex post* kunnen geschieden. In een aantal Nederland omringende landen is het mogelijk voor het parlement om een voorgenomen wet voor te leggen aan de hoogste rechter. In Nederland zou *ex ante* toetsing bijvoorbeeld kunnen worden aangevraagd door een meerderheid in de Eerste Kamer, wier kerntaak het toch al is om voorgenomen wetgeving te toetsen op rechtsstatelijke vraagstukken. Wat betreft *ex post* toetsing zou ervoor kunnen worden gekozen om in de periode dat de wet al wel is aangenomen, maar nog niet in werking is getreden, geselecteerde rechtspersonen toe te staan om de wet aan de hoogste rechter voor te leggen voor abstracte toetsing.

### 8. Vergroot de mogelijkheden van opt-out procedures binnen het civielrecht

Omdat Big Data-processen vaak onder de radar plaatsvinden en mensen zich niet of nauwelijks bewust zijn van het feit dat hun gegevens worden gebruikt en omdat de directe schade die daaruit voortvloeit voor een specifiek individu niet altijd aantoonbaar is, is het vaak lastig voor procespartijen om voldoende massa te creëren om een massaclaim te initiëren ten aanzien van bijvoorbeeld een groot datalek of een partij die op grote schaal onrechtmatig data verwerkt. Daarom zou meer ingezet kunnen worden op opt-out procedures; daartoe is al een aanzet gegeven in het huidige Burgerlijk Wetboek, onder meer door de Wet afwikkeling massaschade in collectieve actie.<sup>17</sup> Toch worden er in ons omringende landen zoals Frankrijk en Duitsland nog meer en bredere mogelijkheden gegeven.<sup>18</sup> Daarnaast wordt zowel in het buitenland als op andere terreinen binnen het Nederlandse recht gewerkt met standaardbedragen voor schadevergoedingen, zoals onder meer voortvloeiend uit een onrechtmatige daad.<sup>19</sup> Een euvel dat procespartijen in het civielrecht aanklaarten als het gaat om schade die voortvloeit uit onrechtmatige gegevensverwerking is dat de bedragen die worden toegekend bij een inbreuk laag zijn, vaak liggend tussen de nul en een paar honderd euro. Dat is voor individuele procespartijen een reden om af te zien van een rechtszaak, en ook professionele partijen die in andere rechtsgebieden collectievebelangenacties opzetten om zo massaschade te claimen, zien daar vooralsnog binnen de datagedreven context van af

14. Conclusie staatsraad advocaat-generaal over exceptieve toetsing, ABRvS 22 december 2017, ECLI:NL:RVS:2017:3557. R. Stolk, 'De legitimiteit van strategisch procederende belangenorganisaties', in: *Strategisch procederen in het bestuursrecht* (Preadvies Jonge VAR-reeks, nr. 16), Den Haag: Boom Juridisch 2017.

15. EHRM 4 december 2015, appl.nr. 47143/06 (*Roman Zakharov/Rusland*), par. 171.

16. Staatscommissie parlementair stelsel, 'Lage drempels, hoge dijken', beschikbaar via [www.staatscommissieparlementairstelsel.nl/documenten/rapporten/samenvattingen/12/13/eindrapport](http://www.staatscommissieparlementairstelsel.nl/documenten/rapporten/samenvattingen/12/13/eindrapport).

17. Wet van 20 maart 2019 tot wijziging van het Burgerlijk Wetboek en het Wetboek van Burgerlijke Rechtsvordering teneinde de afwikkeling van massaschade in een collectieve actie mogelijk te maken (Wet afwikkeling massaschade in collectieve actie), *Stb.* 2019, 130.

18. Kapitalanleger-Musterverfahrensgesetz (KapMuG); M.W.F. Bosters, *Collective redress and private international law in the European Union* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2014. A. Biard en R. Amaro, *Resolving mass claims in France: toolbox and experience*, BACT Working Papers Series 2016/5, beschikbaar via [www.eur.nl/sites/corporate/files/Resolving\\_mass\\_claims\\_Amaro.pdf](http://www.eur.nl/sites/corporate/files/Resolving_mass_claims_Amaro.pdf).

19. [www.rechtspraak.nl/SiteCollectionDocuments/Orientatiepunten-en-afspraken-LOVS.pdf](http://www.rechtspraak.nl/SiteCollectionDocuments/Orientatiepunten-en-afspraken-LOVS.pdf).

omdat zij, zelfs bij een vastgestelde onrechtmatige daad en toegekende strooischade, vaak niet uit de kosten komen. Dit knelpunt zou kunnen worden geadresseerd door het stellen van een standaardschade voor een data-gedreven onrechtmatige daad op € 2.500 per persoon die is geraakt door de inbreuk.

### 9. Breid de mogelijkheden rond het stellen van prejudiciële vragen uit

Uit de gehouden interviews blijkt dat misschien het grootste knelpunt dat rechtspersonen ervaren voor het voeren van zaken in het algemeen belang niet is gelegen in wetgeving maar in een praktisch punt: de kosten. Dit euvel kan op verschillende wijze worden geadresseerd: allereerst zouden de juridische procedures kunnen worden verkort. Momenteel geven partijen aan dat zij vanwege de kosten niet zelden kiezen voor een kort geding. Nadeel van deze benadering is dat de toetsing door de rechter marginaler is. Soms wordt er daarom voor gekozen om eerst een kort geding te starten en pas naderhand een bodemprocedure te beginnen in het geval het kort geding geen succes heeft opgeleverd. Een andere strategie die rechtspersonen daarom bewandelen in zaken in het algemeen belang is het aansturen op prejudiciële vragen. Zo kan in eerste aanleg toch al een uitspraak van de hoogste rechter worden verkregen.

Het stellen van prejudiciële vragen is reeds mogelijk bij het Europees Hof van Justitie<sup>20</sup> en het Europees Hof voor de Rechten van de Mens.<sup>21</sup> Ook in Nederland bestaat de mogelijkheid tot het stellen van prejudiciële vragen aan de Hoge Raad. De in 2012 aangenomen Wet prejudiciële vragen aan de Hoge Raad<sup>22</sup> paste het Eerste Boek van het Wetboek van Burgerlijke Rechtsvordering aan. In een evaluatie die over deze wet is verschenen komt een (zeer) positief beeld naar voren.<sup>23</sup> Omdat de mogelijkheid tot het stellen van prejudiciële vragen leidt tot meer rechtseenheid, minder toekomstige rechtszaken in soortgelijke gevallen en een kortere procedure zijn er plannen om een dergelijke procedure ook in het strafrecht in te voeren.<sup>24</sup> Het is de bedoeling om deze

mogelijkheid via een Innovatiewet Strafvordering vanaf 2021 reeds in experimentvorm mogelijk te maken.<sup>25</sup>

De wetgever zou, om het knelpunt ten aanzien van de kosten te adresseren, kunnen kiezen om de regeling rond prejudiciële vragen verder te verruimen op twee punten. Ten eerste speelt bij het voeren van zaken in het algemeen belang het bestuursrecht een grote rol, mede door de uitspraak van de Hoge Raad in de paspoort-zaak.<sup>26</sup> Daarom zou de regering het initiatief kunnen nemen om de mogelijkheid van prejudiciële vragen, behalve in het strafrecht, ook in het bestuursrecht in te voeren. Ten tweede is de huidige regeling omtrent prejudiciële vragen geënt op zaken waar een rechtsvraag speelt die voor veel andere rechtszaken van belang is. Dit betekent dat er door middel van een prejudiciële beslissing in één keer een antwoord kan worden gegeven op een rechtsvraag die in vele zaken speelt. Zo'n benadering is bij uitstek van toepassing op zaken met een collectief belang en massaclaims. Het is echter niet direct van toepassing op vraagstukken in het algemeen belang. In dergelijke situaties wordt doorgaans één rechtszaak gevoerd, waar een vraagstuk dat raakt aan een algemeen belang door de rechter wordt beoordeeld. Daarom zou kunnen worden overwogen om de procedure rond prejudiciële vragen ook open te stellen voor rechtszaken die worden gevoerd in het algemeen belang.

### 10. Breid de mogelijkheden van *amicus curiae* participatie uit

Zoals genoemd zijn de kosten voor het voeren van een rechtszaak voor procespartijen nu een van de grootste obstakel. Een al dan niet aan het vorige genoemde punt aanvullende optie is het uitbreiden van de mogelijkheden rond *amicus curiae* participatie. Deze vorm is bekend in Angelsaksische landen en wordt ook gebruikt door onder meer het Europees Hof voor de Rechten van de Mens. Er zijn meerdere redenen om derden de mogelijkheid te geven om te interveniëren, bijvoorbeeld om van meer expertise en kennis gebruik te kunnen maken en omdat zaken die draaien rond individuele klachten van individuele belanghebbenden soms ook een groter, maatschappelijk vraagstuk betreffen. Voor de vrienden van het hof betekent het dat zij zich kunnen uitspreken over aan de zaak gerelateerde vraagstukken, zonder dat daarbij proceskosten worden gemaakt. De minister van Rechtsbescherming gaf aan tijdens de Scheltema-lezing: 'Ik denk dat het instrument van meedenkers een bijdrage kan leveren aan een maatschappelijk effectiever bestuursrecht'.<sup>27</sup>

In Nederland is nu reeds tot op zekere hoogte de mogelijkheid van *amicus curiae* participatie in het recht vervat.<sup>28</sup> Momenteel heeft de Raad van State een proef

20. Art. 267 VWEU.

21. Protocol 16 bij het Europees Verdrag voor de Rechten van de Mens.

22. Wet van 9 februari 2012 tot wijziging van het Wetboek van Burgerlijke Rechtsvordering en de Wet op de rechterlijke organisatie in verband met de invoering van de mogelijkheid tot het stellen van prejudiciële vragen aan de civiele kamer van de Hoge Raad (Wet prejudiciële vragen aan de Hoge Raad).

23. I. Giesen e.a., *De Wet prejudiciële vragen aan de Hoge Raad: een tussentijdse evaluatie in het licht van de mogelijke invoering in het strafrecht*, Universiteit Utrecht 2016; beschikbaar via [www.wodc.nl/binaries/2631-volledige-tekst\\_tcm28-124547.pdf](http://www.wodc.nl/binaries/2631-volledige-tekst_tcm28-124547.pdf).

24. Onderwerp Onderzoek prejudiciële vragen Hoge Raad 28 september 2016, beschikbaar via [www.rijksoverheid.nl/documenten/kamerstukken/2017/12/05/wetsvoorstel-tot-vaststelling-van-boek-6-van-het-nieuwe-wetboek-van-strafvordering-bijzondere-regelingen-voorgesteld-artikel-6.2.3.1-e.v.](http://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/05/wetsvoorstel-tot-vaststelling-van-boek-6-van-het-nieuwe-wetboek-van-strafvordering-bijzondere-regelingen-voorgesteld-artikel-6.2.3.1-e.v.)

25. Vijfde voortgangsrapportage modernisering Wetboek van Strafvordering en update van de Contourennota, 9 april 2019, p. 4, beschikbaar via [www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/documenten/kamerstukken/2019/04/09/tk-voortgangsrapportage-modernisering-wetboek-van-strafvordering-en-update-van-de-contourennota](http://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/documenten/kamerstukken/2019/04/09/tk-voortgangsrapportage-modernisering-wetboek-van-strafvordering-en-update-van-de-contourennota).

26. HR 22 mei 2015, ECLI:NL:HR:2015:1296.

27. *NJB* 2019/357.

28. Art. 8:45a Awb.

lopen om de *amicus curiae* participatie uit te breiden. Uit de gehouden evaluatie komt een positief beeld naar voren.

‘Daaruit blijkt dat de inzet van de *amicus curiae* door de procespartijen én amici in het algemeen (zeer) positief wordt gewaardeerd. Zo blijkt dat alle procespartijen zich achter deze ontwikkeling in de praktijk van de Afdeling scharen én het goed vinden dat in hun zaak is gekozen voor de inzet van de *amicus curiae*. Verdeeldheid bestaat onder de procespartijen en amici over het effect op de legitimiteit in de zin van (maatschappelijke) acceptatie van de uitspraak. Het algemene gevoel is dat de *amicus curiae* de legitimiteit versterkt doordat hiermee mogelijk wordt dat met de Afdeling wordt ‘meegedacht’ (participatie) en dat de transparantie van het proces van rechtsvorming door de Afdeling verbetert, mits althans de inzet van de *amicus curiae* wordt gemotiveerd in de uitspraak en hierin tevens wordt aangegeven wie inlichtingen hebben verstrekt en welke rol de inlichtingen hebben gespeeld in de oordeelsvorming. Zo bezien lijkt de relatie tussen de *amicus curiae* en legitimiteit in elk geval gelegen in (meer) participatie en transparantie.’<sup>29</sup>

De wetgever zou ervoor kunnen kiezen om de mogelijkheden voor *amicus curiae* participatie op twee manieren uit te breiden. Ten eerste zou een dergelijke mogelijkheid niet alleen kunnen worden gebruikt in het bestuursrecht, maar ook in het strafrecht en het civielrecht. Ten tweede lijkt er nu nog aarzeling te bestaan ten aanzien van de toepassing van een dergelijke rechtsfiguur, juist als het gaat om zaken in het algemeen belang, zo bleek uit de bovengenoemde evaluatie waarvoor ook staatsraden zijn geïnterviewd.

‘Wat betreft de doelen waarvoor de *amicus curiae* kan worden ingezet, merken wij nog op dat in de interviews door verschillende staatsraden naar voren is gebracht dat de *amicus curiae* aan bepaalde grenzen is gebonden. Zo gaf een staatsraad aan dat in politiek of maatschappelijk zeer gevoelige zaken de inzet van de *amicus curiae* minder voor de hand ligt, omdat dit de bestuursrechter in een ongemakkelijke positie kan brengen. Een andere staatsraad bracht naar voren dat de *amicus curiae* zeer selectief moet worden ingezet om – wat wij maar noemen – ‘reactie-moeheid’ te voorkomen.’<sup>30</sup>

Er zou op dit punt het initiatief kunnen worden genomen om een dergelijke rechtsfiguur wel toe te passen in zaken die draaien om politiek gevoelige materie. Veel Big Data-projecten raken nu juist aan politiek en maat-

schappelijk gevoelige vragen, rechtstatelijke knelpunten en principes van legitimiteit en legaliteit. Omdat de concrete schade of gevolgen van Big Data-projecten vaak lastig te duiden zijn heeft het juist bij rechtszaken ten aanzien van dergelijke projecten de grootste potentiële meerwaarde om gebruik te kunnen maken van informatie van kenniscentra en gespecialiseerde rechtspersonen als vrienden van het hof.

## Conclusie

Nederland transformeert naar een datagedreven samenleving. Het ministerie van Justitie en Veiligheid heeft onderzoek laten verrichten naar de vraag welke juridische aanpassingen nodig zijn om dit proces in goede banen te leiden. In deze bijdrage hebben wij tien aanpassingen aan het huidige procesrecht besproken die ervoor kunnen zorgen dat het Nederlands procesrecht klaar is voor de eenentwintigste eeuw. Daarnaast geeft het rapport ook suggesties ten aanzien van de vraag hoe Big Data-processen zelf beter moeten worden ingekaderd en welke aanpassingen aan het toezicht en de naleving noodzakelijk zijn. Deze twee punten hebben wij in deze bijdrage niet besproken; daarvoor verwijzen wij de lezer naar het eigenlijke rapport.

Van de tien hier besproken reguleringsopties is duidelijk dat zij kunnen worden gezien als een aanbeveling voor beleid, maar dat is niet de primaire functie van de signalering van deze reguleringsopties. Niet alle reguleringsopties zullen op korte termijn haalbaar zijn en sommige reguleringsopties kunnen worden gezien als communicerende vaten. Als er bijvoorbeeld binnen het bestuursrecht goede mogelijkheden zijn om de diverse problemen die bij Big Data kunnen spelen aan te kaarten, dan hoeft er minder te worden ingezet op het versterken van de mogelijkheden binnen het strafrecht en het civielrecht.

Het is in dat licht vooral van belang dat het Nederlandse beleid de voor- en nadelen van alle verschillende opties afweegt, mede gelet op de systematische inbedding van de verschillende rechtsfiguren of beleidsopties in de wettelijke en uitvoeringscontext. Vervolgens zou dan een geschikte combinatie van maatregelen kunnen worden getroffen die tegemoet komt aan de gesignaleerde knelpunten in procedurele waarborgen en toegang tot het recht. Het gaat er uiteindelijk om het rechtstelsel zo vorm te geven dat het burgers en de samenleving als geheel voldoende rechtsbescherming biedt in de datagedreven samenleving.

29. J.C.A. de Poorter, L.A. van Heusden en C.J. de Lange, *De amicus curiae geëvalueerd: Over de eerste indrukken van de inzet van het instrument van de amicus curiae in procedures voor de Afdeling bestuursrecht-spraak*, Den Haag: Raad van State 2018, beschikbaar via [www.njb.nl/Uploads/2018/10/evaluatie-van-de-amicus-curiae.pdf](http://www.njb.nl/Uploads/2018/10/evaluatie-van-de-amicus-curiae.pdf).

30. De Poorter, Van Heusden en De Lange 2018.